

Manuel d'installation , d'utilisation de test et de sécurité



CNL35L
DNL35L

SIL2





LOREME 12, rue des Potiers d'Etain Actipole BORNY - B.P. 35014 - 57071 METZ CEDEX 3
Téléphone 03.87.76.32.51 - Télécopie 03.87.76.32.52
Nous contacter: Commercial@Loreme.fr - Technique@Loreme.fr
Manuel téléchargeable sur: www.loreme.fr

REV 1-25/0615



Sommaire

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr



1 Introduction

1.1 Information générale

Ce manuel contient les informations nécessaires à l'intégration du produit afin d'assurer la sécurité fonctionnelle des boucles connexes. L'ensemble des modes de défaillance et la HFT du module sont précisés dans l'Analyse AMDEC référencée AMDEC CNL35L rev2.XLS

Autres documents Applicables:
- fiche technique CNL35L
- déclaration CE de conformité CNL35L rev2
- Analyse AMDEC CNL35L rev2
- Manuel de configuration CNL35L rev2.x

Les documents mentionnés sont disponibles sur www.loreme.fr

Le montage, l'installation, la mise en service et la maintenance ne peuvent être effectués que par des personnels formés et qualifiés ayant lu et compris les instructions du présent manuel et du manuel de configuration.

Quand il n'est pas possible de corriger les défauts, les appareils doivent être mis hors service, des mesures doivent être prise pour se protéger contre une utilisation accidentelle. Seul le constructeur peut être amené à réparer le produit.

Le non suivi des conseils donnés dans ce manuel peut engendrer une altération des fonctions de sécurité, et causer des dommages aux biens, à l'environnement ou aux personnes.

1.2 Fonction et utilisations prévues

Le CNL35L assure la conversion et l'isolation de signaux analogiques ou de températures issu de cannes pyrométriques.
la retransmission du signal s'effectue sous forme de signal analogique 4...20 mA ou 0...10V.
En option le produit permet la détection de seuils par l'intermédiaire de 4 relais interne.

Les appareils sont conçus, fabriqués et testés en fonction des règles de sécurité applicables.
Ils ne doivent être utilisés que pour les applications décrites et dans le respect des conditions environnementales figurant dans la fiche technique : http://www.loreme.fr/fichtech/CNL35L.pdf

1.3 Normes et directives

Les dispositifs sont évalués conformément aux normes citées ci-dessous:

• Sécurité fonctionnelle selon IEC 61508 , édition 2000:
Standard de la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité électronique.

L'évaluation du matériel a été réalisée par Analyse des Modes de défaillance de leurs Effets et de leur Criticité
(CEI 60812 – Edition 2 - 2006)
permettant de déterminer la proportion de défaillances en sécurité (SFF) de l'appareil.

L'AMDEC s'appuie sur le recueil de données de fiabilité " Modèle universel pour le calcul de la fiabilité prévisionnelle des composants (CEI 62380 - 2004 ou MIL-217F-2) et sur les données constructeur ".

1.4 Information constructeur

LOREME SAS
12, rue des potiers d'étain 57071 Actipole Metz Borny
www.loreme.fr

Conditionneur de signaux analogiques programmable
TYPE : CNL35L et Détecteur de Seuil DNL35L

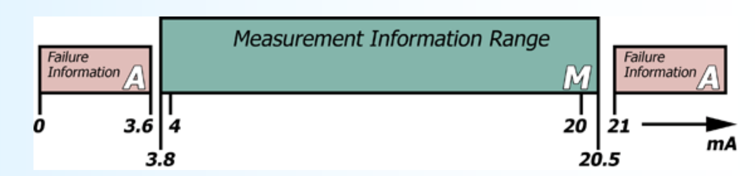


2 Fonction et état de sécurité

2.1 Fonction de sécurité

La fonction de sécurité de l'appareil est remplie, aussi longtemps que la sortie (4 ... 20 mA) reproduit l'image de la mesure d'entrée avec une tolérance de +/-2%. La plage de bon fonctionnement du signal de sortie s'étend de 3.8 mA à 20.5 mA , et que la fonction de détection de seuil n'est pas altérée.

2.2 Position de repli de sécurité (suivant NAMUR NE 43)



L'état de repli de sécurité est défini par un courant de sortie hors de la gamme 3,6mA à 21mA.

- Soit un courant de sortie =< 3,6 mA
- Soit un courant de sortie >= 21 mA

L' application devra impérativement être configurée pour détecter toute valeur de courant hors gamme (=< 3,6 mA et >= 21 mA) et les considérés « Invalides ». De ce fait, dans l'étude AMDEC, cet état est considéré comme "**non dangereux"**.
Le temps de réaction pour toutes les fonctions de sécurité est < 200 ms.

AVERTISSEMENT ! La valeur de repli étant librement programmable, sur le CNL35L, il appartient à l'installateur de vérifier la compatibilité avec la sécurité du process (valeur de repli programmé en sortie usine : 21 mA)

3 Recommandation de sécurité

3.1 Interfaces

Le dispositif est doté des interfaces suivantes:

- les interfaces de sécurité : entrée analogique, sortie analogique, sortie relais

- interfaces non de sécurité : clavier, afficheur, Liaison série RS232 (configuration de l'appareil)

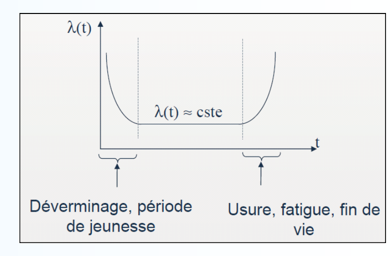
Si l'appareil est équipé de l'option afficheur et clavier, l'accès en configuration locale doit être dé-validé (par la liaison série) pour les applications SIL2.

3.2 Configuration / étalonnage

La configuration de l'appareil est nécessaire pour définir son mode de fonctionnement (type d'entrée, échelle de mesure, valeur de repli) se reporter au manuel de configuration.
Le réétalonnage n'est possible que par retour usine. Aucune modification ne doit être effectué sur le module.

3.3 Durée de vie utile

Evolution du taux de défaillance



Bien qu'un taux de défaillance constant est assumé par l'estimation probabiliste, celui ci ne s'applique que pour la durée de vie utile des composants.
Au-delà de cette durée de vie utile, la probabilité de défaillance s'accroit de manière significative avec le temps.
La durée de vie utile est très dépendante des composants eux même et des conditions de fonctionnement tel que la température, en particulier.
(les condensateurs électrolytiques sont très sensibles à la température de travail)

Cette hypothèse d'un taux de défaillance constant est basée sur la courbe en forme de baignoire, qui montre le comportement typique des composants électroniques.
Par conséquent, la validité de ce calcul est limité à la durée de vie utile de chaque composant.
Il est présumé que les défaillances précoces sont détectées pour un très fort pourcentage durant la période de déverminage constructeur et au cours de la période d'installation, l'hypothèse d'un taux de défaillance constant pendant la durée de vie utile reste donc valide.
Selon la CEI 61508-2, une durée de vie utile, fondée sur le retour d'expérience, doit être prise en considération.
L'expérience a montré que la durée de vie utile est comprise entre 15 et 20 ans, et peut être plus élevé si il n'y a pas de composants a durée de vie réduite dans les fonctions de sécurité (tels que condensateurs électrolytique, relais, mémoire flash, optocoupleur) et si la température ambiante est nettement inférieure à 60 °C.

Remarque :

La durée de vie utile correspond au taux de défaillance aléatoire constant de l'appareil.
La durée de vie effective peut être plus élevée.
! l'intégrateur devra s'assurer que le module n'est plus nécessaire à la réalisation de la sécurité avant sa mise au rebut.

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr



4 Installation , mise en service et remplacement

La capacité de fonctionnement et les courants de signalisation d'erreurs doivent être soumis à un contrôle lors de la mise en service (validation) voir paragraphe : ***" Contrôles périodiques et de mise en service "*** et à des intervalles adéquats préconisés au paragraphe : ***" Périodicité des contrôles "***
Tout appareil ne satisfaisant pas le contrôle de mise en service doit être remplacé.

AVERTISSEMENT !
Aucune maintenance utilisateur ne doit être effectuée, un appareil défectueux doit être remplacé par un matériel neuf de même type. Pour un retour en réparation ou un réétalonnage, il est d'une très grande importance que tous les types de défaillances de l'équipement soit signalées en vue de permettre à l'entreprise de prendre des mesures correctives afin de prévenir les erreurs systématiques.

4.1 Descriptif extérieur

L'afficheur et les voyants d'état
ne sont pas couvert par la fonction de sécurité.
Le clavier interne doit être inhibé en SIL2
pour interdire l'accès au réglages du produit.

Couvercle pivotant
Acces config. RS232
et reglage seuil

Liaison RS232 accessible sous le couvercle pivotant permettant le passage en configuration (n'utiliser que le cordon fourni par LOREME à cet effet)
Attention : le passage en mode configuration fige le courant de sortie (arrêt de la fonction de mesure durant la configuration)
Pour des raisons de sécurité le convertisseur quitte automatiquement le mode configuration après 2 minutes d'inactivité et retourne en mode mesure.

Seul la configuration par la liaison RS232 doit être activée, pour éviter l'entrée en configuration locale par du personnel non autorisé.
(pour les appareils disposant de l'option afficheur)



4.2 Préconisation de raccordements électriques et configuration

Ces informations sont complémentaire au manuel de configuration

- Le module est insensible à la polarité de l'alimentation, il fonctionne indifféremment en alternatif ou en continu.
- Pour un thermocouple distant, s'assurer que la prolongation soit faite avec du câble d'extension ou de compensation du même type que le thermocouple employé, et de la bonne polarité du câble (le non respect peut entrainer des erreurs ou dérive de mesures)
- Pour une sonde PT100 distante, s'assurer que le câble de prolongation utilisé dispose de 3 ou 4 conducteurs de même section pour garantir la meilleur compensation de ligne.
- Pour les entrées mA vérifier le calcul de boucle (tenue en charge) pour éviter une saturation du signal d'entrée.
- Veiller au bon choix du type de capteur dans la configuration.
- Vérifier que l'échelle de température programmé dans l'automate et dans le convertisseur sont identique
- la valeur de repli de la sortie analogique doit être programmé < à 3.6mA ou >= à 21mA (21mA sortie usine)
- les contacts des relais doivent être utilisés de manière à mettre le système en sécurité sur perte d'alimentation du module.

AVERTISSEMENT !

Ne pas dépasser les spécifications de la fiche technique, pour assurer un fonctionnement sûr de la sortie analogique il faut :
- respecter la plage de tension auxiliaire d'alimentation
- respecter la charge maximum dans la boucle avec une marge de 10%.
Attention , un dépassement de charge de la boucle 4...20mA peut empêcher le courant de sortie d'atteindre la valeur maximum ou la valeur de repli. celui-ci pouvant saturer dans la plage de mesure, et mettre le système dans un état dangereux.

4.3 Synoptique interne

Alimentation multiple isolée
Prise console de programmation Mode terminal
M
S2
S1
Sortie 1
Isolation
Entrée mesure Circuit de conversion analogique digital
Microcontrôleur :
-Traitement acquisition
-Interface de programmation RS232
-gestion des sorties analogiques.
Sortie 2
Isolation
Capteur de compensation
127.5 °C
Afficheur 4 Digits
Et réglage seuil
R1
R2
R3
R4

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr



5 Contrôles périodiques et de mise en service

La procédure de test périodique est définie par LOREME et doit être suivie par l'utilisateur final pour assurer et garantir le niveau SIL dans le temps. Les tests périodiques doivent être réalisés en suivant la procédure définie ci dessous et selon la périodicité définie au paragraphe ***" Périodicité des contrôles "***

5.1 Procédure de contrôle

Le test périodique permet la détection d'une éventuelle défaillance interne du produit ainsi que l'étalonnage de la boucle.
Les conditions d'environnement ainsi qu'un temps de chauffe minimum de 5 minutes doivent être respectés.

Test complet du convertisseur et de la chaîne de traitement du signal *(le système est indisponible pendant le test)*

1. Si nécessaire, contourner le système de sécurité et / ou prendre les mesures appropriées, pour assurer la sécurité durant le test
2. Inspecter l'appareil, absence de dommage visible ou de contamination (oxydation)
3. Insérer un milliampèremètre* dans la boucle de sortie
4. Déconnecter le capteur ou le signal d'entrée
5. Vérifier que le courant de sortie passe en valeur de repli (<=3.6mA ou >=21mA)
   (cette fonctionnalité n'est disponible que pour les entrées capteurs et 4...20mA)
6. Connecter un simulateur* à l'entrée du convertisseur
7. Simuler les valeurs de signaux d'entrées appropriées à l'échelle du convertisseur (sur 5 points : 0%, 25%, 50%, 75%, 100%)
   et vérifier que le courant de sortie (4..8..12..16..20mA) soit proportionnel à l'entrée à +/-0.15% près.
8. Vérifier l'enclenchement des seuils (si option sortie relais)
9. Débrancher le simulateur et reconnecter le signal d'entrée du convertisseur
   (vérifier que le courant est dans la gamme de mesure)
9. Retirer le milliampèremètre et refermer la boucle de sortie
10. Après les essais, les résultats doivent être documentés et archivés.

Tout appareil ne satisfaisant pas le contrôle doit être remplacé

*note *: le milliampèremètre et le simulateur doivent être calibré de façon régulière pour ce test*
(selon l'état de l'art et la bonne pratique)

5.2 Périodicité des contrôles

Selon le tableau 2 de la CEI 61508-1 le PFDavg , pour les systèmes fonctionnant à faible sollicitation,
doit être ≥ 10^{-3} à <10^{-2} pour les fonctions de sécurité SIL2 et ≥ 10^{-4} à <10^{-3} pour les fonctions de sécurité SIL3

λ safe detected	λ dangerous detected	λ safe undetected	λ dangerous undetected = PFH	SFF
198 FIT	11 FIT	13 FIT	16 FIT	93.3% (sans relais)
192 FIT	11 FIT	13 FIT	22 FIT	90.75% (avec relais)

conditions : température de 25°C

Valeur du PFDavg en fonction de la périodicité de test

T[Proof] = 1 an	**T[Proof] = 5 ans**	**T[Proof] = 10 ans**	**T[Proof] = 20 ans**
PFDavg=9.60E^{-05}	**PFD**avg=4.80E^{-04}	**PFD**avg=9.60E^{-04}	**PFD**avg=1.9E^{-03}

approximation : PFDavg = λdangerous undetected x T[Proof] /2 (hrs) (erreur engendré par l'approximation < 3%)

Les champs marqués en vert signifie que les valeurs calculées du PFDavg sont dans les limites autorisées pour le SIL2
(en utilisant 10% des ressources de la fonction instrumentée de sécurité, le Tproof peut être augmenté en utilisant une plus grande fraction du SIF)

Récapitulatif :

Probabilité de défaut PFD = 9.20 E^{-5} x Tproof [années]

soit pour Tproof = 10 ans , 10 % de SIF en catégorie SIL2

Remarques :
- les intervalles de test doivent être déterminés en fonction du PFDavg requis par l'intégrateur.

- Le SFF, PFDavg et PFH doit être déterminé pour l'ensemble de la fonction instrumentée de sécurité (SIF)
en s'assurant que les valeurs de courant hors gamme sont bien détectées au niveau système
et qu'elles conduisent effectivement à la position de sécurité.





DECLARATION DE CONFORMITE



REV1
Page 1/1

La société LOREME déclare sous sa seule responsabilité, que le produit :

Désignation: **Conditionneur de signaux analogiques programmable**

Type: **CNL35L**

N° de révision : 2 date : 25/06/2015

Peut être utilisé pour les applications de sécurité fonctionnelle jusqu'à SIL2 selon la Norme IEC61508-2 : 2000 en respectant les consignes de sécurité spécifiées dans le manuel de sécurité.

L'évaluation des défaillances aléatoires et dangereuses pour la sécurité donne les valeurs suivante:

Appareil avec composants du type B , tolérance aux pannes matérielles HFT = 0
valeurs pour le convertisseur seul (cas le plus défavorable avec option relais)

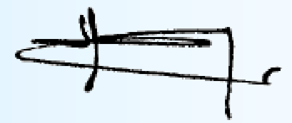
λ safe detected	**λ** dangerous detected	λ safe undetected	λ dangerous undetected = PFH	**SFF (1)**	**PFD**avg T[Proof] **= 1 an**	**PFH**
192 FIT(2)	11 FIT(2)	13 FIT(2)	22 FIT(2)	90.75%	$9.60E^{-05}$	$2.2E^{-08}$ 1/h

(1) selon AMDEC CNL35L rev2 *établi avec "ALD MTBF calculator" : http://www.aldservice.com/*
(2) FIT = Failure rate (1/h)

Le manuel de sécurité donne les probabilités de défaillance des capteurs associés (pt100 et thermocouple) pour permettre l'évaluation d'une boucle complète.

Metz, le : 25/06/2015

Signé au nom de LOREME ; M. Dominique Curulla



LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr



AMDEC Détaillée

Contexte

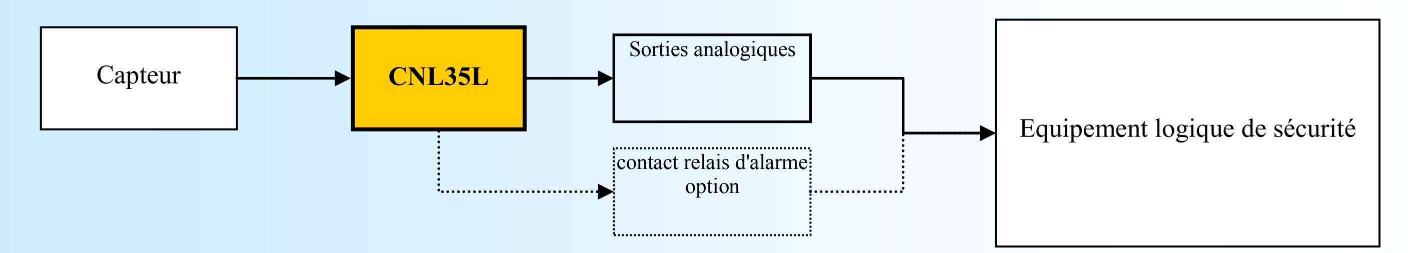
Ce document est l'Analyse des Modes de Défaillance, de leur Effet et de leur Criticité (AMDEC) du composant CNL35L de la société LOREME.
Outre la caractérisation des informations nécessaires pour la sûreté de fonctionnement (en particulier pour les calculs de disponibilité et de constitution de stock de pièces de rechange), cette étude permet de répondre aux exigences de la norme CEI-61508 en identifiant et quantifiant les défaillances dangereuses du composant, permettant ainsi d'interagir sur la conception afin d'éviter ou de réduire ces risques.

Circonstances de l'analyse

Cette étude a été réalisée dans le but de vérifier l'aptitude du convertisseur CNL35L à être utilisé dans des applications de sécurité SIL2

Périmètre de l'analyse

Le composant concerné comprend un ensemble de composants électroniques faisant l'acquisition de signaux d'entrée issus de capteurs et restituant un signal de sortie analogique (4..20mA) avec ou sans relais d'alarme.
Généralement, un convertisseur est interfacé entre un capteur et un équipement de protection, désigné « Equipement logique de sécurité»



Caractérisation du composant

Le convertisseur CNL35L est un sous-système de type « B » [CEI61508-2-§ 7.4.3.1.2] :
Les modes de défaillances des composants nécessaires à la réalisation de la fonction de sécurité sont bien définis.
Le comportement du convertisseur dans des conditions d'anomalie est entièrement déterminé.
Le convertisseur bénéficie d'un retour d'expérience dans de nombreuses applications de sécurité.

Défaillance en sécurité

[CEI61508-4-§3,6.8] Défaillance en sécurité: Défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.
Une défaillance en sécurité est une défaillance qui n'est pas dangereuse. On parle aussi de défaillance sûre.

SFF [CEI61508-2-§7.4.3.1.1-d] La proportion de défaillances en sécurité d'un sous-système appelé SFF (Safe Failure Fraction) est définie par le rapport entre la somme des probabilités de défaillances en sécurité λS plus les défaillances dangereuses détectées λDD sur la somme des probabilités de défaillances fonctionnelles total du sous-système (ensemble des « défaillances en sécurité » λS et des « défaillances dangereuses » λD).

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}$$

Défaillance dangereuse

[CEI61508-4-§3,6.7] Défaillance dangereuse : défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction. On parle aussi de panne non sûre.

Conditionneur de signaux analogiques programmable
TYPE : CNL35L et Détecteur de Seuil DNL35L



Analyse fonctionnelle

Le convertisseur se compose :
d'un étage d'alimentation
d’un étage d’entrée convertisseur analogique numérique
d'un microcontrôleur (linéarisation, compensation et mise à l'échelle du signal ainsi que le traitement des alarmes)
d'un étage d'isolation (transmission du signal)
d'un étage de sortie (amplificateur de courant)
et de relais d'alarmes.

Définition de l’évènement redouté

Pour le convertisseur **CNL35L,** l'événement redouté (c'est-à-dire la défaillance dangereuse, telle que définie dans la section précédente) est l'émission d’un courant de sortie erroné :
Soit un courant de sortie erroné de plus de 2% par rapport à la demande du procédé.
Soit un courant de sortie, bloqué à une valeur, tel qu’il ne peut prendre une valeur de repli de sécurité:
courant de sortie bloqué dans une gamme > 3,6mA ou < 21mA
ou l'impossibilité de transmettre une alarme.

Définition de la position de repli de sécurité

L’état de repli de sécurité est défini par un courant de sortie hors de la gamme 3,6mA – 21mA.
Soit un courant de sortie =< 3,6 mA
Soit un courant de sortie >= 21 mA
La valeur de repli du convertisseur devra impérativement être programmé pour l'une de ces valeurs.
Le programme d’application de l’« Equipement logique de sécurité » devra impérativement être configuré
pour détecter toute valeur de courant hors gamme (=< 3,6 mA et >= 21 mA) et les considérées « Invalides ».
De ce fait, dans l’étude AMDEC, cet état est considéré comme non dangereux.

Hypothèses d'étude

Les taux de défaillance des composants sont considérés constants sur toute la durée de vie du système.
L'évaluation des caractéristiques de sûreté d'un module fait intervenir un certain nombre d'hypothèses :
Seul l'aspect matériel est traité. L'aspect sûreté de fonctionnement du logiciel n'est pas abordé.
(la sureté du logiciel est prise en compte durant la phase de développement, de vérification et de validation de la conception dans les procédures d'assurance qualité, ainsi que dans le choix des outils de développement.)
Seules les défaillances catalectiques sont prises en compte : Défaillances franches, soudaines et non prévisibles.
Ne sont pas considérées, les défauts qui pourraient être dus à :
- des erreurs de conception,
- à des défauts de lot en production,
- à l’environnement (interférences électriques, cycles de température, vibrations) ;
- des erreurs humaines en fonctionnement ou en maintenance,
(des précautions sont prises pour les éviter : gestion d'une L.O.F.C. (liste des opérations de fabrication et de contrôle)
Ne sont traitées que les pannes simples. Les défauts de soudure, qui sont généralement dus à une non qualité détectable en fin de fabrication par un déverminage spécifique, ne sont pas pris en compte.
Tous les aspects touchant aux fonctionnalités spécifiques à la phase de mise sous tension ne sont pas traités.

Taux de défaillance

Les taux de pannes élémentaires des composants du convertisseur CNL35L sont disponible dans le document :
AMDEC CNL35L rev2.XLS disponible sur demande.

Etabli avec " ALD MTBF calculator "   selon : MIL-HDBK-217F Notice 2 Electronic Reliability Prediction.

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Techni-



Annexe 2 :
Utilisation des données de L'AMDEC et information complémentaire sur les capteurs de température.

Le convertisseur de mesure raccordé à un capteur de température devient un assemblage.
Par conséquent, lors de l'utilisation des résultats de l'AMDEC dans une évaluation SIL,
le taux de défaillance des capteurs (pt100 ou thermocouple) doit être pris en considération pour le calcul de la fonction instrumentée de sécurité (SIF)
Ci-dessous le récapitulatif des modes de défaillance et leur fréquence pour les PT100 et les thermocouples en fonction du type de raccordement et de l'environnement dans lequel ils sont utilisés.

Taux de défaillance typiques de thermocouples et PT100 avec fils d'extension (capteur déporté)

type d'élément de mesure	taux de défaillance (FIT)
thermocouple en environnement de faible stress	1000
thermocouple en environnement de stress élevé	20000
Pt100 montage 2/3 fils en environnement de faible stress	475
Pt100 montage 2/3 fils en environnement de stress élevé	9500
Pt100 montage 4 fils en environnement de faible stress	500
Pt100 montage 4 fils en environnement de stress élevé	10000

Taux de défaillance typiques de thermocouples et PT100 sans fils d'extension (capteur avec transmetteur incorporé)

type d'élément de mesure	taux de défaillance (FIT)
thermocouple en environnement de faible stress	100
thermocouple en environnement de stress élevé	2000
Pt100 montage 2/3 fils en environnement de faible stress	48
Pt100 montage 2/3 fils en environnement de stress élevé	960
Pt100 montage 4 fils en environnement de faible stress	50
Pt100 montage 4 fils en environnement de stress élevé	1000

Répartition typique des modes de défaillance pour les thermocouples

Type de défaillance	Avec fils d'extension	Raccordement direct Sans extension
Circuit ouvert	90%	95%
Court circuit	5%	4%
Dérive *	5%	1%

** le phénomène de dérive des thermocouples est essentiellement du au vieillissement*

Répartition typique des modes de défaillance pour les sonde PT100

Type de défaillance	Avec fils d'extension	Raccordement direct Sans extension
Circuit ouvert	78%	79%
Court circuit	2%	3%
Dérive	20%	18%

La répartition du taux de défaillance dépend légèrement du type de raccordement des pt100 (2,3,4 fils)

Les conditions de stress sont : des vibrations importantes sur le process et ou des cycles fréquent de température, ces phénomènes pouvant causer des fissures du substrat et des ruptures de soudure sur les fils de raccordement.



Annexe 3 : termes et définitions.

SIL signifie “Security Integrity Level”, c’est-à-dire le niveau d’intégrité de la sécurité. La notion de SIL a été introduite dans la norme IEC61508 et elle est reprise dans les normes dérivées de l’IEC61508, telles que la norme IEC61511 relative aux systèmes instrumentés de sécurité (SIS) pour les process et l’IEC62061 pour les systèmes de sécurité à électronique programmable pour les machines.
Lorsque l’on veut réaliser une installation de sécurité, il faut commencer par évaluer le risque (sa dangerosité, sa fréquence d’occurrence), ce qui conduit à définir les exigences de sécurité que l’on attends du SIS, c’est-à-dire son SIL.
En définitive, le SIL définit le niveau de fiabilité du SIS. Il existe deux manières de définir le SIL, selon que le système de sécurité fonctionne en mode de faible sollicitation ou si au contraire s’il fonctionne en continu ou à forte sollicitation. Il existe 4 niveaux de SIL (notés SIL1 à SIL4) plus le SIL est élevé, plus la disponibilité du système de sécurité est élevée.
Pour les **systèmes de sécurité fonctionnant en mode de faible sollicitation**,
on parle de probabilité moyenne de défaillance sur sollicitation PFD_{avg} (Probability of Failure on Demand) sur une période de 10 ans.
La relation entre les niveaux SIL et le PFDavg est la suivante :
SIL 4 : PFDavg compris entre 10^{-5} et 10^{-4}
SIL 3 : PFDavg compris entre 10^{-4} et 10^{-3}
SIL 2 : PFDavg compris entre 10^{-3} et 10^{-2}
SIL 1 : PFDavg compris entre 10^{-2} et 10^{-1}
Pour les **systèmes de sécurité fonctionnant en mode de sollicitation élevée,** on parle de PFH, probabilité de défaillance dangereuse par heure. La relation entre les niveaux SIL et le PFH est la suivante :
SIL 4 : PFH compris entre 10^{-9} et 10^{-8}
SIL 3 : PFH compris entre 10^{-8} et 10^{-7}
SIL 2 : PFH compris entre 10^{-7} et 10^{-6}
SIL 1 : PFH compris entre 10^{-6} et 10^{-5}

Échelle des niveaux SIL

	Sollicitations du SIS		
SIL*	rares PFD**	fréquentes PFH***	Facteur de réduction du risque
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$	10 000 à 100 000
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$	1 000 à 10 000
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$	100 à 1 000
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$	10 à 100

** Safety Integrity level, niveau d'intégrité de la sécurité*
***Probability of Failure on low Demand, probabilité d'avoir une défaillance (pour réaliser la fonction de sécurité prévue) au moment d'une sollicitation*
****Probability of a dangerous Failure per Hour ou Probability of Failure on High demand, probabilité d'une défaillance dangereuse par heure*

Abréviation	Description
HFT	Tolérance matérielle; capacité d'un module fonctionnel de continuer l'exécution d'une fonction sollicitée en présence d'erreurs
MTBF	Temps moyen entre deux défaillances
MTTR	Temps moyen entre la survenance d'une erreur dans un appareil ou un système et la réparation
PFD	Probabilité de défaillances menaçantes d'une fonction de sécurité en cas de sollicitation
PFDavg	Probabilité moyenne de défaillances menaçantes d'une fonction de sécurité en cas de sollicitation
SIL	Safety Integrity Level (niveau d'intégrité de sécurité) ; la norme internationale IEC 61508 définit quatre Safety Integrity Level (SIL1 à SIL4). Chaque niveau correspond à une plage de probabilité pour la défaillance d'une fonction de sécurité. Plus le Safety Integrity Level des systèmes de sécurité est élevé, plus la probabilité qu'ils n'exécutent pas les fonctions de sécurité sollicitées est faible.
SFF	Partie de défaillances non dangereuses, partie de défaillances ne présentant pas de potentiel pour mettre le système de sécurité dans un état de fonctionnement dangereux ou inadmissible.
TProof	Contrôle répétitif permettant de détecter des défaillances dans un système de sécurité.
XooY	Classification et description du système de sécurité en termes de redondance et de procédé de sélection appliqué. "Y" indique la fréquence à laquelle la fonction de sécurité est exécutée (redondance). "X" détermine le nombre de canaux qui doivent fonctionner correctement.
λsd et λsu	λsd Safe detected et λsu Safe undetected Taux de défaillance ne présentant aucun danger . Une défaillance ne présentant aucun danger (safe failure) est donnée quand le système de mesure passe à l'état sûr défini ou au mode de signalisation d'erreurs sans sollicitation émanant du procédé.
λdd et λdu	λdd Dangerous detected et λdu Dangerous undetected Taux de défaillance dangereuse généralement, une défaillance dangereuse est donnée quand le système de mesure est mis dans un état dangereux ou entravant le fonctionnement.
λdu	λdu Dangerous undetected Une défaillance dangereuse non détectée est donnée lorsque le système de mesure ne passe ni à l'état sûr défini, ni au mode de signalisation d'erreurs en cas de sollicitation émanant du procédé.

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Techni-